



Oslo kommune
Byrådsavdeling for finans

Justis- og beredskapsdepartementet
Postboks 8005 Dep.
0030 OSLO

Dato: 05.04.2019

Deres ref:
18/6579

Vår ref (saksnr):
201900574-4

Saksbeh:
Atle H. Hjelkerud, 412 90 275

Arkivkode:
040

**OSLO KOMMUNES HØRINGSUTTALELSE - NOU 2018: 14 IKT-SIKKERHET I
ALLE LEDD OG UTKAST TIL LOV SOM GJENNOMFØRER NIS-DIREKTIVET I
NORSK RETT**

Oslo kommune viser til felles høring om NOU 2018: 14 IKT-sikkerhet i alle ledd og utkast til lov som gjennomfører NIS-direktivet i norsk rett. Høringen er datert 21.12.2018, men Oslo kommune mottok høringen først 17.01.2019.

Etter forespørsel, har Oslo kommune fått forlenget høringsfrist til 05.04.2019.

1. Innledning

Oslo kommune viser til Justis- og beredskapsdepartementets høringsbrev 21.12.2018 om NOU 2018: 14 IKT-sikkerhet i alle ledd og utkast til lov som gjennomfører NIS-direktivet i norsk rett.

Den teknologiske utviklingen gjør at samfunnet endrer seg. Det er større avhengigheter mellom virksomheter, sektorer og land. IKT-infrastrukturen blir derfor stadig viktigere å sikre. Endret teknologi og en raskere utvikling medfører at risikobildet er endret og utfordringene må håndteres. Holte-utvalgets mandat var å vurdere behovet for rettslige og organisatoriske endringer innen IKT-sikkerhetsområdet.

EUs NIS-direktiv pålegger medlemsstatene å sørge for et visst minstenivå for landets IKT-sikkerhet ved å lage en strategi for sikkerhetsarbeidet, etablere en IKT-sikkerhetsberedskapsenhet (CSIRT) og pålegge operatører og leverandører av samfunnsviktige tjenester IKT-sikkerhetskrav og varslingsplikt ved alvorlige IKT-sikkerhetshendelser. NIS-direktivet har altså som formål å styrke IKT-sikkerheten i EU.

Denne høringen omfatter både NOU 2018: 14 IKT-sikkerhet i alle ledd (Holte-utvalget) og utkast til lov som skal kunne gjennomføre NIS-direktivet i norsk rett. Høringen omfatter imidlertid kun gjennomføring av de delene av direktivet som krever lovendring. Dette omfatter krav til at tilbydere av samfunnsviktige tjenester og tilbydere av enkelte digitale tjenester gjennomfører hensiktsmessige og forholdsmessige sikkerhetstiltak, basert på en risikovurdering. Tjenestetilbyderne skal også varsle om alvorlige hendelser. Det skal føres tilsyn med etterlevelsen, og mangelfull etterlevelse kan sanksjoneres.

Det gjøres oppmerksom på at NIS-direktivet foreløpig ikke er tatt inn i EØS-avtalen, men det legges til grunn at direktivet vil bli tatt inn etter hvert.

Oslo kommune vil innledningsvis understreke viktigheten av at krav til IKT-sikkerhet må balanseres mot informasjonens tilgjengelighet og brukervennligheten for innbyggerne. Dette må være førende når nye krav til IKT-sikkerhet vurderes og foreslås. Den norske befolkning har høy digital modenhet og forventer gode digitale tjenester i kontakten med det offentlige. Regjeringen har som mål at innbyggere og næringslivet bare skal behøve å rapportere samme informasjon til det offentlige én gang. Vi understreker derfor viktigheten av at digitale løsninger tilrettelegger for gjenbruk og deling av informasjon, samtidig som at sikkerheten naturligvis må være tilstrekkelig.

2. NOU 2018: 14 IKT-sikkerhet i alle ledd

Holte-utvalget har i NOU 2018: 14 IKT-sikkerhet i alle ledd gitt fem anbefalinger for endringer innen IKT-sikkerhetsområdet. Utvalget anbefaler at det vedtas en ny lov om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning, at det stilles krav om IKT-sikkerhet ved alle offentlige anskaffelser, at det etableres et nasjonalt IKT-sikkerhetssenter, at det gis tydeligere regulering av og ansvar for tilkoblede produkter og tjenester, og at Justis- og beredskapsdepartementet må utøve et tydeligere lederskap for nasjonal IKT-sikkerhet.

Oslo kommune støtter i all hovedsak anbefalingene fra Holte-utvalget. Det anses å være behov for mer helhetlig regulering av krav til IKT-sikkerhet, krav til varsling og sikkerhetssenter.

Norske virksomheter, både offentlige og private, må forholde seg til flere regelverk som regulerer krav til IKT-sikkerhet. Både sikkerhetsloven, personopplysningsloven, sektorspesifikke regelverk og lovutkastet som gjennomfører NIS-direktivet i norsk rett regulerer krav til IKT-sikkerhet. De gir også regler for varsling, men i ulike situasjoner. Varslene skal i tillegg sendes til ulike myndigheter.

Oslo kommune mener derfor at det er et stort behov for tydeligere lederskap for nasjonal IKT-sikkerhet. Oslo kommune støtter også forslaget fra Holte-utvalget om å nedsette et eget lovutvalg som skal utrede en lov som stiller krav om IKT-sikkerhet til alle norske virksomheter. Oslo kommune mener imidlertid at dette lovutvalget bør få et enda videre mandat, slik at utvalget kan se på den helhetlige reguleringen av krav om IKT-sikkerhet.

Når det gjelder Holte-utvalgets anbefaling om å etablere et nasjonalt IKT-sikkerhetssenter, vil dette kunne støtte opp under et mer helhetlig IKT-sikkerhetsregime. Et nasjonalt IKT-sikkerhetssenter vil, slik Holte-utvalget vurderer det, kunne koordinere og dele informasjon når uønskede digitale hendelser skal håndteres, styrke samarbeidet mellom offentlig og privat sektor og styrke innovasjonsevnen innenfor IKT-sikkerhet. Senteret vil også kunne samle kompetanse og være et sentralt kontaktpunkt for råd og veiledning til virksomheter. Et IKT-sikkerhetssenter vil kunne tillegges oppgaver som ingen offentlige myndigheter har ansvar for i dag. Oslo kommune mener imidlertid at et IKT-sikkerhetssenters rolle må vurderes opp mot andre tilsyns- og rådgivningsmyndigheter, som Datatilsynet. Det er flere forhold ved et slikt IKT-sikkerhetssenter som må utredes.

Oslo kommune er videre enig i utvalgets anbefaling om å stille krav om innebygd sikkerhet i produkter og tjenester som er koblet til internett. Det er imidlertid viktig å minne om at ansvaret for sikkerheten vil ligge hos offentlig sektor i tjenester de tilbyr, uansett om det er en ekstern leverandør som har utviklet tjenestene.

3. Utkast til lov som gjennomfører NIS-direktivet i norsk rett

Høringen omfatter også utkast til lov som gjennomfører NIS-direktivet i norsk rett. I høringsbrevet er høringsinstansene bedt om å gi innspill på følgende spørsmål:

- I hvilken grad arbeides det per i dag systematisk med IKT-sikkerhet i din virksomhet? Følges for eksempel visse standarder for sikkerhetsstyring eller internkontroll?
- Beskriv hvilke positive konsekvenser forslaget til gjennomføring av NIS-direktivet vil få for din virksomhet.
- Beskriv hvilke negative konsekvenser forslaget til gjennomføring av NIS-direktivet vil få for din virksomhet.
- Er din virksomhet per i dag underlagt krav til IKT-sikkerhet og varsling? Hvilket regelverk – lover, forskrifter eller annet – er det som stiller slike krav?
- Bør en slik lov som foreslås i denne høringen vedtas selv om vi ikke er forpliktet til det i henhold til EØS-avtalen?

Oslo kommune består av 52 virksomheter og hver virksomhet er selv ansvarlig for arbeidet med IKT-sikkerhet i sin egen virksomhet. Samtlige virksomheter er omfattet av krav til IKT-sikkerhet og varsling etter Oslo kommunes interne regelverk. Flere av virksomhetene er også underlagt krav til IKT-sikkerhet og varsling etter nasjonale og sektorspesifikke regelverk, blant annet i helsesektoren. Av denne grunn vil det være store forskjeller i hvordan arbeidet med IKT-sikkerhet utføres i de ulike virksomhetene. Det vil også være store forskjeller mellom virksomhetene når det gjelder positive og negative konsekvenser av forslaget til gjennomføring av NIS-direktivet.

Oslo kommune mener det er positivt at det vedtas en lov som gjennomfører NIS-direktivet selv om Norge per dags dato ikke er forpliktet til det etter EØS-avtalen. Bakgrunnen for dette er at det anses å være et behov for å gi lovregler som vil øke IKT-sikkerheten.

Oslo kommune mener imidlertid at loven som er foreslått må revideres før den vedtas. Holte-utvalgets anbefalinger bør innarbeides i lovforslaget, slik at kravene etter loven vil gjelde for alle offentlige virksomheter, og ikke bare samfunnskritiske virksomheter. Dette vil imidlertid kreve ekstra bevilgninger, slik at lovkravene kan etterleves på en god måte.

Sikkerhetsloven stiller krav om sikring av informasjonssystemer som behandler skjermingsverdig informasjon eller som i seg selv har avgjørende betydning for grunnleggende nasjonale funksjoner. NIS-direktivet stiller på sin side krav til sikring av nettverk og informasjonssystemer som brukes for å levere den samfunnsviktige tjenesten. I høringsnotatet legges det til grunn at det kan være sammenfall mellom disse to tilnærmingene, men ikke nødvendigvis. Sikkerhetskravene etter personopplysningsloven har likhetstrekk med kravene etter lovutkastet, da de begge stiller krav om risikovurdering og iverksetting av tekniske og organisatoriske tiltak. For enkelte sektorer vil det være sektorspesifikke regelverk som regulerer krav til IKT-sikkerheten. I lovutkastets § 5 er det presisert at den sektorspesifikke loven skal benyttes dersom kravene til sikkerhet og varsling minst tilsvarer lovutkastet.

Oslo kommune mener det skaper uoversiktliggjhet at krav til IKT-sikkerhet er regulert i ulike lover. Oslo kommune mener det hadde vært fordelaktig om krav til IKT-sikkerhet i større grad ble harmonisert og samlet i ett regelverk. Et slikt regelverk bør bygges opp slik at det stilles generelle minimumskrav som gjelder alle virksomheter og særlige krav som gjelder virksomheter som faller innenfor sikkerhetslovens bestemmelser og lovutkastets bestemmelser. På sikt bør også krav om IKT-sikkerhet som er regulert i sektorspesifikke lover samles i ett regelverk, slik at kravene som stilles harmoniseres.

4. Økonomiske og administrative konsekvenser

I høringsnotatet er det vist til at det på nåværende tidspunkt ikke er klart hvilke virksomheter som vil bli omfattet av loven. Samtidig fremgår det at lovutkastet vil kunne innebære økte kostnader for berørte virksomheter. Når det gjelder eventuelle økte kostnader, har departementet lagt til grunn at offentlige myndigheter må ta av eksisterende budsjetter for å dekke merarbeidet, og det vil være opp til den enkelte sektor å omprioritere eller tilføre friske midler dersom eksisterende budsjetterrammer ikke er tilstrekkelig.

Oslo kommune mener det er svært vanskelig å anslå hvilke økonomiske og administrative konsekvenser den foreslåtte loven vil få for kommunen, ettersom det ikke er klart hvilke virksomheter som vil bli omfattet av loven. De økonomiske kostnadene kan potensielt bli av en størrelsesorden det er umulig å finne dekning for innenfor eksisterende budsjetterrammer, spesielt i kommunesektoren. Oslo kommune mener derfor det må være en klar forutsetning at offentlige myndigheter blir kompensert for merkostnadene lovendringen medfører, slik at virksomhetene gis reell mulighet til å oppfylle kravene på en god måte. Dette gjelder både engangskostnaden med å tilpasse seg regelverket når et nettverk eller et informasjonssystem underlegges loven og de løpende kostnadene ved å vedlikeholde, oppgradere og drifte disse. Kommunene vil ha utfordringer med å etterleve de nye lovkravene dersom ikke det vil følge med bevilgninger til nødvendige tilpasninger.

Oslo kommune er en stor kommune med mange virksomheter, og det vil ta tid å implementere nye lovkrav. Det gjelder spesielt ettersom mer konkrete vilkår for hvilke virksomheter som skal omfattes ikke foreligger per dags dato. Det understrekes et behov for en tilstrekkelig lang overgangsperiode, særlig for de virksomheter som ikke har vært underlagt loven tidligere, og en klar forventning om at statlige myndigheter bistår med nødvendig veiledning og rådgivning i prosessen.

Det må også påpekes at det er stor ulikhet i kommunenes gjennomføringsevne. Store kommuner vil lettere kunne gjennomføre endringer i krav til IKT-sikkerhet, sammenlignet med små kommuner. Dette betinger imidlertid tilstrekkelige ressurser og tid til å implementere endringer. Det er viktig å se helheten i kommunesektoren og behovet for at staten bidrar til at alle kommuner evner å gjennomføre endringer.

Som nevnt innledningsvis, understreker Oslo kommune viktigheten av at krav til IKT-sikkerhet må balanseres mot informasjonens tilgjengelighet og brukervennligheten for innbyggerne. Den norske befolkning har høy digital modenhet og forventer gode digitale tjenester i kontakten med det offentlige. Oslo kommune støtter regjeringens mål om at innbyggere og næringslivet bare skal behøve å rapportere samme informasjon til det offentlige én gang. Vi understreker viktigheten av at digitale løsninger tilrettelegger for gjenbruk og deling av informasjon, samtidig som at sikkerheten naturligvis må være tilstrekkelig.

Med hilsen

Arild Sundberg
kommunaldirektør

Randi Blystad
konst. seksjonssjef

Godkjent elektronisk